وزارت علوم، تحقیقات و فناوری
دانشگاه شهید مدنی آذربایجان

رساله
جهت اخذ مدرک دکتری
رشته ریاضی محض

محاسبه خمهای بیضوی در خانواده هایی از پیچش درجه دوم

استاد راهنما
دکتر فرضعلی ایزدی

استاد مشاور
دکتر قربانعلی حقیقت دوست بناب

پژوهشگر
کامران نبردی

دیماه ۱۳۹۲
تبریز - ایران


بسم الله الرحمن الرحيم

ماحصل آموخته هایم راتقدیم می کنم

به آنان که مهر آسمانی شان آرام بخش آلام زمینی ام است

به استوارترین تکیه گاهم، دستان پر مهر پدرم

به آبی ترین نگاه زندگیم، چشمان آبی مادرم

که هرچه آموختم در مکتب عشق شما آموختم وهرچه بکوشم قطره ای از دریای بیکران مهربانیتان راسپاس نتوانم بگویم.

و

تقدیم به همسرم عزیزم،

که سایه مهربانیش سایه سار زندگیم است، او که اسوه صبر و تحمل بوده و مشکلات مسیر رابرایم تسهیل نمود.

الهی...

چون توانستم، ندانستم، و چون که دانستم، نتوانستم.

دانایی ده که از راه نیفتم، و بینایی ده که در چاه نیفتم.

هر که را عقل دادی، چه ندادی؟ و هر که را عقل ندادی، چه دادی؟!

ابوجهل، از کعبه می آید! و ابراهیم از بتخانه! کار به عنایت بود، باقی بهانه.

با صنع تو هر مور چه رازی دارد با شوق تو هر سوخته تازی دارد.

ای خالق ذوالجلال نومید مکن آن را که به درگهت نیازی دارد.

وقتی جز خدا هیچ ندارم... همه چیز دارم و

وقتی جز خدا همه چیز دارم... هیچ ندارم.

سپاس گزاری...

سپاس خداوندی را که به من آموخت در لحظه‌های شادی شکرگزار باشم و فراموش نکنم، تمام داشته‌ها و دانسته‌هایم از لطف بی‌منت اوست و آموخت که در لحظه‌های اندوهم صبور باشم که همه‌ی غم‌ها رفتنی است و سربلند کسی است که مطیع تقدیر و حکمت الهی باشد.

اینک به پاس لطف الهی که این پایان‌نامه به سرانجام رسیده است برخود واجب می‌دانم از حمایت‌های بی‌دریغ، بذل توجه و مساعدت‌های استاد راهنمای گرامیم جناب آقای دکتر **فرضعلی ایزدی** سپاسگزار نمایم . دلسوزی، تلاش و کوشش ایشان در تعلیم و تربیت و انتقال معلومات و تجربیات ارزشمند در کنار رابطه ای صمیمی و دوستانه با بنده و ایجاد فضایی دلنشین برای کسب علم و دانش و درک شرایط، حقیقتاً قابل ستایش است. اینجانب برخود وظیفه می دانم در مقام شاگردی از زحمات و خدمات ارزشمند ایشان تقدیر و تشکر نمایم.

از جناب آقای دکتر **قربانعلی حقیقت دوست**، که مشاوره و مطالعه این پایان‌نامه را به عهده گرفتند، کمال تشکر را دارم. از آقایان دکتر **علی سرباز جانفدا** ، دکتر **جعفر امجدی** و دکتر **اسماعیل عابدی** نیز سپاسگزارم که قبول زحمت فرموده و داوری این تحقیق را برعهده گرفتند.

از همسر مهربانم که در این مدت با قبول مشکلات و تحمل رنجهای بسیار با فراهم آوردن محیطی آرام و دلنشین، موجب شد که با آرامش خاطر این مقطع تحصیلی را به پایان برسانم سپاسگزارم.

در خاتمه، دست بوس پدر و مادر عزیزم هستم که دعاهای خیر ایشان ضامنی مطمئن در تمام مراحل زندگی ام بوده است.

کامران نبردی
دیماه ۱۳۹۲

فهرست مطالب

لیست جداول

لیست تصاویر

چکیده

فرض کنید n یک عدد صحیح بصورت $n = p^۴ + q^۴ = r^۴ + s^۴$ است. یک خانواده جدید از خمهای بیضوی بصورت $E_n : y^۲ = x^۳ - nx$ تعریف می کنیم. نشان می دهیم رتبه این خانواده حداقل برابر ۳ است. با فرض درست بودن حدس زوجیت، ثابت می شود که حداقل رتبه برای این خانواده برابر ۴ است. درستی حدس سیلورمن در رابطه با پیچش درجه دوم یک خم بیضوی را برای این خانواده بررسی می کنیم. در انتها، معادله دیوفانتی درجه چهارم $X^۴ + Y^۴ = ۲(U^۴ + V^۴)$ را برای اولین بار با دو روش مختلف حل کرده و نشان می دهیم بیشمار جواب صحیح برای این معادله وجود دارد. به کمک جوابهای این معادله یک خانواده جدید از خمهای بیضوی با رتبه حداقل ۵ تعریف می کنیم.

کلمات کلیدی: معادله دیوفانتی، خم بیضوی، رتبه، حدس زوجیت، پیچش درجه دوم، حدس سیلورمن، حدس BSD

پیشگفتار

یکی از اساسی ترین سؤالات در رابطه با خمهای بیضوی، چگونگی ساختار گروهی آن روی میدان $\mathbb{Q}$ است. بنا به قضیه مردل-ویل [۱]، گروه نقاط یک خم بیضوی روی یک میدان اعداد [۲] ، متناهی مولد [۳] است. می زور[۴]، ۱۵ گروه متناهی ارائه کرد و نشان داد بازاء هر خم بیضوی دلخواه روی $\mathbb{Q}$، زیر گروه تاب[۵] فقط با یکی از این ۱۵ حالت یکریخت است. در حالی که محاسبه زیر گروه تاب هر خم بیضوی کار چندان دشواری نیست، بدست آوردن مولدهای مستقل قسمت آزاد[۶] آن که تعداد آنها رتبه [۷] نامیده می شود بسیار چالش برانگیز است. بطور کلی هیچ راه حل کلی که بتوان رتبه همه خمها را به کمک آن محاسبه کرد وجود ندارد. باور کلی بر این است: بازاء هر عدد طبیعی M، می توان یک خم بیضوی پیدا کرد که رتبه آن برابر M باشد. متاسفانه دلایل کافی برای اثبات این حدس وجود ندارد.

در تلاش برای یافتن خمهای با رتبه بالا، ریاضیدانان بسیاری، خانواده های مختلفی از خمهای بیضوی را درنظر گرفته اند . یکی از این خانواده ها بصورت

$$E_n : \ y^2 = x^3 - nx$$

است. مقالات متعددی در رابطه با رتبه این خانواده منتشر شده است. در هر یک از آنها، حالات مختلفی برای n در نظر گرفته و با توجه به ویژگیهای آن در صدد پیدا کردن رتبه بالا بوده اند. از جمله این تلاشها می توان به [۳۴، ۳۱، ۳۰، ۲۳، ۱۷، ۱۵، ۱۲، ۴، ۱] اشاره کرد. نتایج حاصل از تلاش این ریاضیدانان در فصل دوم ذکر شده است.

در این رساله دو کار عمده صورت گرفته است. ابتدا، فرض می کنیم که n یک عدد طبیعی است بطوریکه

[۱] Mordell-Weil theorem
[۲] number field
[۳] finitely generated
[۴] Mazur
[۵] torsion
[۶] free part
[۷] rank

$n = p^۴ + q^۴ = r^۴ + s^۴$ که در آن p، q، r و s اعداد صحیح هستند. اویلر [۱۱]، نشان داد بیشمار عدد صحیح وجود دارد که در این رابطه صدق می کنند. وی این اعداد را پارامتری کرده است. ما در این رساله نخست، خانواده بالا را بازای چنین n هایی درنظر گرفته و به نتایج جدیدی درباره رتبه این خانواده دست پیدا می کنیم. کار بعدی صورت گرفته در این رساله عبارت است از حل معادله دیوفانتی درجه چهارم $X^۴ + Y^۴ = ۲(U^۴ + V^۴)$ ، که ما آن را برای اولین بار با دو روش متفاوت حل می کنیم. سرانجام خانواده $E_n : y^۲ = x^۳ - nx$ را دوباره درنظر گرفته، که این بار n، تابعی از جوابهای این معادله دیوفانتی است. برای رسیدن به اهداف مورد نظر، مطالب این رساله در چهار فصل تنظیم شده است که در ادامه توضیح مختصری را در مورد هر فصل ذکر می کنیم.

فصل اول: مطالب مورد نیاز از نظریه اعداد شامل نماد لژاندر[۱]، مانده درجه دوم[۲] و معادلات دیوفانتی[۳] در بخش اول این فصل بیان شده اند. چندین معادله دیوفانتی که در فصل دوم برای رسیدن به نتایج مطلوب به آنها نیاز داریم، در این فصل ذکر و در وجود و یا عدم وجود جواب برای آنها بحث شده است. در بخش دوم، مطالبی از هندسه جبری شامل تعاریف فضای آفین[۴] و فضای تصویری[۵] را آورده ایم. تعریف یک خم بیضوی روی یک میدان دلخواه و ویژگیهای اساسی آن در بخش سوم بیان می شوند. در بخش چهارم چند روش مختلف برای محاسبه رتبه یک خم بیضوی را معرفی می کنیم.

فصل دوم: ابتدا خانواده $E_n : y^۲ = x^۳ - nx$ را درنظر می گیریم که در آن $n = p^۴ + q^۴ = r^۴ + s^۴$. سپس با استفاده از چند ویژگی برای عدد n، قضیه اساسی فصل دوم (قضیه ۱.۴.۲) را ثابت می کنیم. به عبارت دیگر نشان می دهیم که رتبه این خانواده حداقل برابر ۳ است. با فرض اینکه حدس زوجیت[۶] درست باشد، نشان می دهیم بازای n های فرد حداقل رتبه این خانواده برابر ۴ است. با ارائه مثالهای عددی این فصل را به پایان می رسانیم.

فصل سوم: در فصل سوم تلاش ما بر این است که درستی حدس سیلورمن[۷] را برای این خانواده ثابت کنیم. تمام نتایج مبتنی بر نظریه اعداد می باشد.

فصل چهارم: در این فصل یک معادله دیوفانتی درجه چهارم بصورت $X^۴ + Y^۴ = ۲(U^۴ + V^۴)$ را در نظر

[۱] Legendre symbol
[۲] quadratic residue
[۳] Diophantine equation
[۴] affine space
[۵] projective space
[۶] parity conjecture
[۷] Silverman's conjecture

گرفته و برای اولین بار آن را با دو روش مختلف حل می کنیم. در روش اول متناظر با هر نقطه از خم بیضوی $y^۲ = x^۳ - ۳۶x$ یک جواب برای معادله بدست می آوریم. در روش دوم بر اساس یک جواب اولیه و یک رابطه بازگشتی نشان می دهیم که می توان بیشمار جواب صحیح بدست آورد. پس از حل این معادله، خانواده $E_n : y^۲ = x^۳ - nx$ را درنظرگرفته که در آن n تابعی از جوابهای این معادله است.

از این رساله مقالات زیر استخراج شده است:

[1] Izadi, F., Khoshnam, F., and Nabardi, K., *Sums of two biquadrates and elliptic curves of rank* ≥ 4, Mathematical Journal of Okayama University, 56 (2014), 51-63.

[2] Izadi, F., and Nabardi, K., *Diophantine equation* $X^4+Y^4=2(U^4+V^4)$, Mathematica Slovaca, Accepted.

[3] Izadi, F., and Nabardi, K., *On Silverman's conjecture for a family of elliptic curves*, Bulletin of the Iranian Mathematical Society, Accepted.

[4] Izadi, F., and Nabardi, K., *A family of elliptic curves with rank* ≥ 5, Submitted.

فصل ۱
مقدمات

این فصل شامل چهار بخش است. در بخش اول مطالبی از نظریه اعداد و معادلات دیوفانتی را یادآوری می کنیم که در این رساله نقش اساسی دارند. برای نمونه چندین معادله دیوفانتی در قالب مثال و یا لم حل شده است که اثبات نتایج اصلی فصل دوم بر آنها استوار است. در بخش دوم مفاهیم مقدماتی هندسه جبری تعریف می شود. نظریه خمهای بیضوی را در بخش سوم آورده ایم. بخش چهارم به نحوه پیدا کردن رتبه یک خم بیضوی اختصاص دارد.

۱.۱ مطالبی از نظریه اعداد

تعریف ۱.۱.۱. (مانده درجه دوم) عدد صحیح a را یک مانده درجه دوم به پیمانه $m \in \mathbb{N}$ می نامیم هرگاه معادله همنهشتی $x^2 \equiv a \pmod{m}$ دارای جواب باشد. در صورتی که این معادله همنهشتی فاقد جواب باشد آنگاه a را یک نامانده درجه دوم به پیمانه m می نامیم.

تعریف ۲.۱.۱. (نماد لژاندر) هرگاه $p > 2$ یک عدد اول و a عددی صحیح باشند آنگاه نماد لژاندر را که به شکل $\left(\frac{a}{p}\right)$ نمایش داده می شود به صورت زیر تعریف می کنیم:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{هرگاه } a \text{ یک مانده درجه دوم به پیمانه } p \text{ باشد} \\ -1 & \text{هرگاه } a \text{ یک نامانده درجه دوم به پیمانه } p \text{ باشد} \\ 0 & p \mid a \end{cases}$$

قضیه ۱.۱.۱. *فرض کنید p یک عدد اول و a و b اعداد صحیح دلخواه اند. آنگاه:*

(*الف*) $a \equiv b \pmod{p} \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$؛

(*ب*) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$؛

(ج) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$؛

(د) $\left(\frac{۱}{p}\right) = ۱$؛

(ه) $\left(\frac{-۱}{p}\right) = (-۱)^{(p-۱)/۲}$؛

(و) $\left(\frac{-۱}{p}\right) = ۱ \iff p \equiv ۱ \pmod{۴}$.

برهان. به [[۱۳]، گزاره ۵.۱.۲] مراجعه کنید. ■

قضیه ۲.۱.۱. *بازای همه اعداد اول فرد p داریم:*

$$\left(\frac{۲}{p}\right) = \begin{cases} ۱ & p \equiv \pm ۱ \pmod{۸}, \\ -۱ & p \equiv ۳,\ ۵ \pmod{۸}. \end{cases}$$

برهان. واضح است که،

$$(۱+i)^۲ = ۲i.$$

همچنین، بازای عدد اول p داریم:

$$(۱+i)^p = ۱ + \binom{p}{۱} i + \binom{p}{۲} i^۲ + \cdots + i^p.$$

با درنظر گرفتن معادله بالا به پیمانه $p\mathbb{Z}[i]$، داریم:

$$(۱+i)^p \equiv ۱ + i^p \pmod{p\mathbb{Z}[i]}.$$

از طرف دیگر،

$$\begin{aligned} (۱+i)^p &= (۱+i)(۱+i)^{p-۱} \\ &= (۱+i)((۱+i)^۲)^{(p-۱)/۲} \\ &= (۱+i)(۲i)^{(p-۱)/۲} \\ &= i^{(p-۱)/۲}(۱+i)۲^{(p-۱)/۲}. \end{aligned}$$

از اینرو،

$$i^{(p-۱)/۲}(۱+i)۲^{(p-۱)/۲} \equiv ۱ + i^p \pmod{p\mathbb{Z}[i]}. \qquad (۱.۱)$$

حال مقادیر مختلف $p \pmod{۸}$ را درنظر می گیریم.

(الف) اگر $p \equiv ۱ \pmod{۸}$، آنگاه $i^p = i$. همچنین، $i^{(p-۱)/۲} = ۱$. از اینرو، معادله (۱.۱) بصورت زیر در می آید

$$(۱+i) \equiv (۱+i)۲^{(p-۱)/۲} \pmod{p\mathbb{Z}[i]},$$

پس،

$$۱ \equiv ۲^{(p-۱)/۲} \pmod{p\mathbb{Z}[i]}.$$

از اینرو $۲^{(p-۱)/۲} \equiv ۱ \pmod{p}$. حال با توجه به قضیه ۱.۱.۱ قسمت (ب)، داریم $\left(\frac{۲}{p}\right) = ۱$.

(ب) اگر $p \equiv -۱ \pmod{۸}$، آنگاه $i^p = -i$. همچنین، $i^{(p-۱)/۲} = -i$. از اینرو، (۱.۱) بصورت زیر در می آید:

$$(۱-i) \equiv -i(۱+i)۲^{(p-۱)/۲} \pmod{p\mathbb{Z}[i]},$$

و از آن نتیجه می شود:

$$۱ \equiv ۲^{(p-۱)/۲} \pmod{p\mathbb{Z}[i]}.$$

از اینرو $۲^{(p-۱)/۲} \equiv ۱ \pmod{p}$ و بنابراین $\left(\frac{۲}{p}\right) = ۱$.

(ج) اگر $p \equiv ۳ \pmod{۸}$، آنگاه $i^p = -i$. بعلاوه، $i^{(p-۱)/۲} = i$. از اینرو،

$$\begin{aligned}(۱-i) &\equiv i(۱+i)۲^{(p-۱)/۲} \pmod{p\mathbb{Z}[i]},\\ -i(۱+i) &\equiv i(۱+i)۲^{(p-۱)/۲} \pmod{p\mathbb{Z}[i]},\\ -۱ &\equiv ۲^{(p-۱)/۲} \pmod{p\mathbb{Z}[i]}.\end{aligned}$$

چون $۲^{(p-۱)/۲} \not\equiv ۱ \pmod{p}$، لذا $\left(\frac{۲}{p}\right) = -۱$.

(د) اگر $p \equiv ۵ \pmod{۸}$، آنگاه $i^p = i$. همچنین، $i^{(p-۱)/۲} = -۱$. از اینرو،

$$\begin{aligned}(۱+i) &\equiv -۱(۱+i)۲^{(p-۱)/۲} \pmod{p\mathbb{Z}[i]},\\ -۱ &\equiv ۲^{(p-۱)/۲} \pmod{p\mathbb{Z}[i]}.\end{aligned}$$

لذا، $\left(\frac{۲}{p}\right) = -۱$ و به این ترتیب اثبات کامل می شود.

■

لم ۱.۱.۱. *فرض کنید m یک عدد صحیح است. فرض کنید p یک عدد اول فرد است بطوریکه $\gcd(p,\ m) = ۱$. فرض کنید $p \mid x^۲ + my^۲$ که در آن $\gcd(x,\ y) = ۱$. دراینصورت $\left(\frac{-m}{p}\right) = ۱$.*

برهان. اگر $p \mid y$، آنگاه $p \mid x^۲$ و از اینرو، $p \mid x$. رابطه اخیر یک تناقض است، زیرا $\gcd(x,\ y) = ۱$. از اینرو $\gcd(p,\ y) = ۱$. بنابراین y دارای یک وارون ضربی به پیمانه p مانند $z_۰$ است. داریم:

$$x^۲ + my^۲ \equiv ۰ \pmod{p}.$$

از اینرو،

$$(z_۰x)^۲ + m \equiv ۰ \pmod{p},$$

پس $\left(\frac{-m}{p}\right) = ۱$. ■

مجموع مربعات

بنا به تعریف، عدد صحیح مثبت n را می توانیم بصورت مجموع دو مربع بنویسیم هرگاه معادله

$$n = x^۲ + y^۲,$$

دارای جواب صحیح $x_۰$ و $y_۰$ باشد. بازای هر عدد صحیح x، واضح است که $x^۲ \equiv ۰,\ ۱ \pmod{۴}$. از اینرو،

$$\forall x,\ y \in \mathbb{Z} \qquad x^۲ + y^۲ \equiv ۰,\ ۱,\ ۲ \pmod{۴}.$$

نتیجه ۱.۱.۱. *اعداد صحیح به شکل $۴m + ۳$ بصورت مجموع دو مربع نیستند.*

قضیه ۱.۱.۳. *فرض کنید p یک عدد اول است. آنگاه p مجموع دو مربع است اگر و تنها اگر*

$$p = ۲ \text{ یا } p \equiv ۱ \pmod{۴}.$$

برهان. با توجه به توضیحات بالا، اعداد اول $p \equiv ۳ \pmod{۴}$ نمی توانند بصورت مجموع دو مربع باشند. همچنین داریم $۲ = ۱^۲ + ۱^۲$. حال نشان می دهیم اعداد اول $p \equiv ۱ \pmod{۴}$ را می توانیم بصورت مجموع دو مربع بنویسیم.

فرض کنید $p \equiv ۱ \pmod{۴}$، قرار می دهیم $N = [\sqrt{p}]$. آنگاه $N < \sqrt{p} < N + ۱$. بنا به قضیه ۱.۱.۱

قسمت (و)، -۱ یک مانده مربعی به پیمانه p است، لذا یک عدد صحیح مانند i وجود دارد بطوریکه $i^۲ \equiv -۱ \pmod{۴}$. مجموعه A را بصورت زیر تعریف می کنیم:

$$A = \{ (j,\ k) \mid j,\ k \in \mathbb{Z},\ j,\ k \in [۰,\ N] \}.$$

فرض کنیم B مجموعه کامل مانده ها به پیمانه p است،

$$B = \{\overline{۰},\ \overline{۱}, \cdots ,, \overline{p-۱}\ \}.$$

نگاشت $f : A \to B$ را با ضابطه $f(x,\ y) = x + iy$ درنظر می گیریم. B دارای p عضو و A دارای $(N+۱)^۲$ عضو است و می دانیم $(N+۱)^۲ > p$. لذا، تابع f یک به یک نیست. از اینرو، بازای دو زوج متمایز $(x_۱,\ y_۱)$ و $(x_۲,\ y_۲)$ از A داریم:

$$x_۱ + iy_۱ \equiv x_۲ + iy_۲ \pmod{p}.$$

قرار می دهیم $a = x_۱ - x_۲$ و $b = y_۱ - y_۲$. واضح است که a و b هر دو صفر نیستند. از رابطه بالا واضح است، $a^۲ \equiv i^۲ b^۲ \pmod{p}$. از اینرو، $p \mid a^۲ + b^۲$. از طرف دیگر $|a| \le N$ و $|b| \le N$ و بنابراین

$$۰ < a^۲ + b^۲ \le ۲N^۲ < ۲p.$$

از اینرو، $p = a^۲ + b^۲$. ■

قضیه ۴.۱.۱. *فرض کنید $n = a^۲ + b^۲$. فرض کنید عدد اول $q \equiv ۳ \pmod{۴}$ در تجزیه n به عوامل اول ظاهر شده است. آنگاه*

(الف) $q \mid a$ و $q \mid b$.

(ب) *توان q در تجزیه n به عوامل اول، زوج است.*

برهان.

(الف) فرض کنید $q \nmid a$. لذا $(q,\ a) = ۱$ و بنابراین a دارای یک وارون ضربی به پیمانه q است. یعنی،

$$\exists\, s \in \mathbb{Z}, \qquad sa \equiv ۱ \pmod{q}.$$

با ضرب طرفین همنهشتی $a^۲ + b^۲ \equiv ۰ \pmod{q}$ در $s^۲$، داریم:

$$(sb)^۲ = s^۲ b^۲ \equiv -s^۲ a^۲ \equiv -۱ \pmod{q}.$$

از اینرو، ۱− یک مانده مربعی به پیمانه q است. این نتیجه بنا به قضیه ۱.۱.۱ قسمت (و)، یک تناقض است. به همین ترتیب ثابت می شود $q \mid b$.

(ب) چون $q \mid a$ ، $q \mid b$ و $n = a^۲ + b^۲$، لذا $q^۲ \mid n$. با تقسیم طرفین رابطه اخیر بر $q^۲$ داریم:

$$\frac{n}{q^۲} = (\frac{a}{q})^۲ + (\frac{b}{q})^۲.$$

از اینرو، عدد صحیح $n_۱ = \frac{n}{q^۲}$ بصورت مجموع دو مربع است. اگر $q \mid n_۱$، نتیجه می گیریم $q^۲ \mid n_۱$ و با ادامه روند قبل، می توان استدلال کرد که توان q زوج است.

■

معادلات دیوفانتی

مطالعه معادلات دیوفانتی عبارت است از پیدا کردن جوابهای معادلات چندجمله ای و یا دستگاههای معادلات در حلقه اعداد صحیح، اعداد گویا، و یا بطور کلی در حلقه اعداد جبری. این مبحث یکی از قدیمی ترین شاخه های نظریه اعداد و در واقع ریاضیات است، نوشته های بابلیان باستان، چینیها، مصریان، و یونانیان شاهدی بر این ادعا است. یکی از جذابیتهای این موضوع این است که بر خلاف صورت ساده مسائل، در اغلب حالات، حل بسیار مشکلی دارند.

فرض کنید $(x_۱, y_۱, z_۱)$ یک جواب صحیح برای معادله دیوفانتی

$$x^۲ + y^۲ = z^۲ \qquad (۲.۱)$$

است. با فرض زوج بودن $x_۱$ و $y_۱$ نتیجه می شود که $z_۱$ نیز زوج است ولذا می توانیم جواب ساده تری بصورت $(x_۰, y_۰, z_۰) = (x_۱/۲, y_۱/۲, z_۱/۲)$ برای آن پیدا کنیم. از اینرو ما همواره جوابهایی را برای معادلات دیوفانتی در نظر می گیریم که به ساده ترین حالات باشند و در واقع از جواب دیگری مشتق نشده باشند. ما این جوابها را، جوابهای اولیه [۱] می نامیم. با یک استدلال مبتنی بر نظریه اعداد مقدماتی می توان نشان داد که جوابهای اولیه معادله (۲.۱) بصورت

$$x = ۲ab, \qquad y = b^۲ - a^۲, \qquad z = b^۲ + a^۲ \qquad (۳.۱)$$

[۱] primitive solution